# Beleidsuitgangspunten VCSW

**www.vcsw.nl**

VCSW B.V.
Postbus 90422
2509 LK Den Haag

Erkend Adviesbureau

# Beleidsuitgangspunten VCSW

1. Informatiebeveiliging is één van de belangrijke bedrijfsrisico's voor VCSW. De directie stelt het beleid vast, beoordeelt de risico's, stelt de maatregelen vast en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen.

2. VCSW conformeert zich m.b.t. de informatiebeveiliging aan de van toepassing zijnde wetgeving.

3. De 'best practices' van de norm NEN-ISO/IEC 27001 en de Algemene Verordening Gegevensbescherming (AVG) welke per 25 mei 2018 de privacy richtsnoeren van de Autoriteit Persoonsgegevens (AP), het voormalige College Bescherming Persoonsgegevens (CBP) vervangt, vormen, voor zover zij bijdragen aan de informatiebeveiliging van VCSW, het uitgangspunt voor de te definiëren maatregelen. Dit is een bedrijfseconomische afweging.

4. VCSW beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken. Ook dit is een bedrijfseconomische afweging.

5. Vertrouwen is voor VCSW een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. VCSW gaat er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.

6. Alleen maatregelen, waarvan handhaving goed mogelijk is, komen in aanmerking voor implementatie.

7. Het HRM-beleid is mede gericht op het verbeteren van de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening. Tijdens functioneringsgesprekken vindt hiervan evaluatie plaats.

8. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.

9. Aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan het basisbeveiligingsniveau (BBN).

10. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.

11. Ontwikkeling en aanschaf van en onderhoud op informatiesystemen geschieden volgens een standaardaanpak met een formele acceptatie door de gebruikersorganisatie. (zie de daarvoor bestemde procedure investerings- en wijzigingsvoorstellen)

12. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten en personeel conform de verwerkersovereenkomst te waarborgen.

13. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van VCSW.

14. Gegevensverstrekking extern gebeurt op basis van ‘need to know’. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.

15. VCSW en haar medewerkers treffen maatregelen om te voorkomen, dat informatie in handen van derden terechtkomt.

16. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.

17. In de productieomgeving wordt gewerkt met geautoriseerde versies van (legale) programmatuur.

18. Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.

19. Er is een proces om incidenten adequaat af te handelen en hier ‘lessons learned’ uit te trekken.

20. Er zijn calamiteitenplannen en voorzieningen om de continuïteit van de informatievoorziening te waarborgen.

21. Bij de geautomatiseerde informatievoorziening zijn stringente scheidingen aangebracht tussen de test-/ontwikkelomgeving, de acceptatie/testomgeving en de productieomgeving. Van belang hierbij is dat er geen vertrouwelijke productiegegevens buiten de goed beveiligde productieomgeving komen.

22. Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.

23. Open source software wordt alleen gebruikt indien deze voldoet aan open standaards en afkomstig is van betrouwbaar geachte leveranciers of bronnen.